What is claimed is:

1. A method for authenticating a payment service being used in a transaction comprising:

generating on a payment device a first verification value unique to the transaction wherein said first verification value is derived from data comprising a first data value and a second data value;

communicating a payment record from the payment device to a point of sale terminal, wherein the payment record comprising the first verification value and payment data;

communicating the payment record from the point of sale terminal to a service provider computer;

generating a second verification value on the service provider computer, wherein the second verification value is generated solely from data residing on the service provider computer; and

disapproving the transaction when the first verification value does not equal the second verification value.

2. The method of claim 1 wherein said first data value comprises:

a primary account number for the payment service.

3. The method of claim 1 wherein said first data value comprises:

a unique identification number for the payment device.

4. The method of claim 1 wherein said first data value comprises:

a unique identification number for the service provider.

5. The method of claim 1 wherein said second data value comprises:

an application transaction counter.

6. The method of claim 1 wherein said second data value comprises:

a cryptogram.

7. The method of claim 1 wherein said second data value comprises:

a digital signature.

8. The method of claim 1 wherein said second data value comprises:

a value derived from the payment data.

9. The method of claim 1 wherein said first verification value is derived from data further comprising:

a service code which identifies the payment service; and

an expiration date for the payment service.

10. The method of claim 1 wherein the application transaction counter is incremented with any non-zero value with each executed transaction.

11. The method of claim 1 wherein the payment record further comprises an application transaction counter.

12. The method of claim 11 further comprising:

storing the application transaction counter in memory accessible by the service provider computer.

13. The method of claim 1 wherein the payment device communicates the payment record to the point of sale terminal via wireless communications.

14. A method of dynamically creating a verification value for a transaction comprising:

creating a base record comprising a first data value and a second data value for a payment service being used in the transaction;

splitting the base record into a first field and a second field;

encrypting the first field using a first encryption key;

performing an exclusive-OR (XOR) operation on the encrypted first field and the second field to produce a first result;

encrypting the first result using a second encryption key to produce a second result;

decrypting the second result using a decryption key to produce a third result;

encrypting the third result using a third encryption key to produce a fourth result;

sequentially extracting each value between 0 and 9 from the most-significant digit to the least-significant digit of the fourth result to produce a fifth result;

sequentially extracting and subtracting hexadecimal A from each value between hexadecimal A and hexadecimal F from the most-significant digit to the least-significant digit of the fourth result to produce the sixth result;

concatenating the fifth result and the sixth result to produce a seventh result; and

selecting one or more values from the seventh result as the card verification value.

15. The method of claim 14 wherein the first encryption key, the second encryption key, and the third encryption key are equivalent.

16. The method of claim 14 wherein the decryption key differs from the first encryption key.

17. The method of claim 14 wherein the decryption key differs from each of the first encryption key, the second encryption key, and the third encryption key.

18. The method of claim 14 wherein the base record is 128-bits in length.

19. The method of claim 14 wherein said first data value comprises:

a primary account number for the payment service.

20. The method of claim 14 wherein said first data value comprises:

a unique identification number for the payment device.

21. The method of claim 14 wherein said first data value comprises:

a unique identification number for the service provider.

22. The method of claim 14 wherein said second data value comprises:

an application transaction counter.

23. The method of claim 14 wherein said second data value comprises:

a cryptogram.

24. The method of claim 14 wherein said second data value comprises:

a digital signature.

25. The method of claim 14 wherein said second data value comprises:

a value derived from the payment data.

26. The method of claim 14 wherein said first verification value is derived from data further comprising:

a service code which identifies the payment service; and

an expiration date for the payment service.

27. The method of claim 14 wherein the base record further comprises padding characters to extend the base record to a predetermined length.

28. The method of claim 14 wherein the first encryption key, the second encryption key, the decryption key, and the third encryption key are derived from data residing on the payment device.

29. A system for verifying a transaction comprising:

a first electronic device with a payment service deployed thereon;

a second electronic device in communication with the first electronic device wherein the second electronic device receives a payment record from the first electronic device, the payment record comprising an account number for the payment service and a first verification value generated on the first electronic device;

a service provider system in communication with the second electronic device wherein the service provider computer independently generates a second verification value and disapproves the transaction where the first verification value and the second verification value are not equal.

30. The system of claim 29 wherein the first electronic device is an integrated circuit card.

31. The system of claim 29 wherein the first electronic device is a personal digital assistant.

32. The system of claim 29 wherein the first electronic device is a cell phone.

33. The system of claim 29 wherein the first electronic device is a device comprising:

a microprocessor; and

means for communicating with the second electronic device.

34. The system of claim 29 wherein the first electronic device communicates with the second electronic device via radio frequency waves.

35. The system of claim 29 wherein the electronic device communicates with the second electronic device via infrared frequency waves.

36. The system of claim 29 wherein the electronic device communicates with the second electronic device via laser communication.

37. The system of claim 29 wherein the second electronic device is comprised of:

means for communicating with the first electronic device; and

a terminal.

38. The system of claim 37 wherein the second electronic device is further comprised of a hardware security key.